

Claim Amendments

1. (Original) A method comprising
transferring an authenticated code module to a private memory; and
executing the authenticated code module stored in the private memory in
response to determining that the authenticated code module stored in the private
memory is authentic.
2. (Original) The method of claim 1 further wherein transferring comprises
transferring a number of bytes specified by an operand from a memory.
3. (Currently Amended) The method of claim 1 further comprising
configuring a cache memory of ~~the~~ a processor to operate like as a random
access memory,
wherein transferring comprises storing the authenticated code module in the
cache memory.
4. (Original) The method of claim 3 further comprising invalidating the cache
memory prior to storing the authenticated code module in the cache memory.
5. (Original) The method of claim 3 further comprising locking the cache
memory to prevent lines of authenticated code module from being replaced.
6. (Original) The method of claim 1 further comprising determining whether
the authenticated code is authentic based upon a digital signature of the
authenticated code module.

7. (Original) The method of claim 1 further comprising
obtaining a first value from the authenticated code module stored in the
private memory;
computing a second value from the authenticated code module; and
determining that the authenticated code module is authentic in response to
the first value and the second value having a predetermined relationship.

8. (Original) The method of claim 1 further comprising
retrieving a key,
decrypting a digital signature of the authenticated code module with the key to
obtain a first value,
hashing the authenticated code module to obtain a second value; and
executing the authenticated code module in response to the first value and
the second value having a predetermined relationship.

9. (Original) The method of claim 8 wherein
decrypting comprises using the key to RSA-decrypt the digital signature, and
hashing comprises apply a SHA-1 hash to the authenticated code module to
obtain the second value.

10. (Currently Amended) The method of claim 8 further comprising retrieving
the key from ~~the~~ a processor used to execute the authenticated code module.

11. (Original) The method of claim 8 further comprising retrieving the key
from a chipset.

12. (Currently Amended) The method of claim 8 further comprising retrieving the key ~~from~~ from a token.

13. (Original) The method of claim 1 wherein transferring comprises receiving the authenticated code module from a machine readable medium.

14. (Original) A computing device, comprising
a chipset;
a memory coupled to the chipset;
a machine readable medium interface to receive an authenticated code module from a machine readable medium;
a private memory coupled to the chipset; and
a processor to transfer the authenticated code module from the machine readable medium interface to the private memory and to authenticate the authenticated code module stored in the private memory.

15. (Original) The computing device of claim 14, wherein the chipset comprises a memory controller coupled to the memory and a separate private memory controller coupled to the private memory.

16. (Original) The computing device of claim 14, wherein
the chipset comprises a key, and
the processor authenticates the authenticated code module stored in the private memory based upon the key of the chipset.

17. (Original) The computing device of claim 14, wherein
the processor comprises a key and authenticates the authenticated code
module stored in the private memory based upon the key of the processor.

18. (Original) The computing device of claim 14, further comprising
a token coupled to the chipset, the token comprising a key, wherein
the processor authenticates the authenticated code module stored in the
private memory based upon the key of the token.

19. (Currently Amended) A computing device, comprising
a chipset;
a machine readable medium interface to receive an authenticated code
module from a machine readable medium; and
a processor coupled to the chipset via a processor bus, the processor to
transfer the authenticated code module from the machine readable medium interface
to a private memory of the processor, and to authenticate the authenticated code
module stored in the private memory, and to execute the authenticated code module
stored in the private memory after authenticating the authenticated code module.

20. (Original) The computing device of claim 19, wherein the private memory
is coupled to the processor via a dedicated bus.

21. (Original) The computing device of claim 19, wherein the private memory
is internal to the processor.

22. (Original) The computing device of claim 19, wherein the private memory comprises internal cache memory of the processor.

23. (Original) The computing device of claim 19, further comprises other processors coupled to the chipset via the processor bus, wherein the processor further locks the processor bus to prevent the other processors from altering the authenticated code module.

24. (Original) A computing device, comprising
a memory;
a chipset comprising a memory control that defines a portion of the memory as private memory;
a machine readable medium to receive an authenticated code module from a machine readable medium; and
a processor to transfer the authenticated code module from the machine readable medium interface to the private memory and to authenticate the authenticated code module stored in the private memory.

25. (Original) The computing device of claim 24, wherein the chipset comprises a memory controller coupled to the memory and a separate private memory controller coupled to the private memory.

26. (Original) The computing device of claim 24, wherein
the chipset comprises a key, and
the processor authenticates the authenticated code module stored in the private memory based upon the key of the chipset.

27. (Original) The computing device of claim 24, wherein
the processor comprises a key and authenticates the authenticated code
module stored in the private memory based upon the key of the processor.

28. (Original) The computing device of claim 24, further comprising
a token comprising a key, wherein
the processor authenticates the authenticated code module stored in the
private memory based upon the key of the token.

29. (Original) A machine readable medium comprising one or more
instructions that in response to being executed result in a computing device
transferring an authenticated code module to a private memory associated
with a processor; and
executing the authenticated code module stored in the private memory in
response to determining that the authenticated code module stored in the private
memory is authentic.

30. (Original) The machine readable medium of claim 29, wherein the one or
more instructions in response to being executed result in the computing device
determining whether the authenticated code is authentic based upon a digital
signature of the authenticated code module.

31. (Original) The machine readable medium of claim 29, wherein the one or more instructions in response to being executed result in the computing device

- obtaining a first value from the authenticated code module stored in the private memory;
- computing a second value from the authenticated code module; and
- determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship.

32. (Original) The machine readable medium of claim 29, wherein the one or more instructions in response to being executed result in the computing device

- retrieving an asymmetric key;
- decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value;
- hashing the authenticated code module to obtain a second value; and
- initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship.

33. (Original) The machine readable medium of claim 29, wherein the one or more instructions comprises a launch instruction that in response to being executed results in the computing device

- retrieving an asymmetric key;
- decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value;
- hashing the authenticated code module to obtain a second value; and

initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship.

34. (Original) The machine readable medium of claim 33, wherein the one or more instructions in response to being executed result in the computing device receiving the authenticated code module via a machine readable medium interface.